# UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

INFORMATION ASSOCIATED WITH ONE IP ADDRESS THAT IS STORED AT PREMISES CONTROLLED BY GODADDY.COM, LLC

Case No. 1:23MJ 42

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the ______ District of Arizona, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☑ evidence of a crime;

☑ contraband, fruits of crime, or other items illegally possessed;

☑ property designed for use, intended for use, or used in committing a crime;

□ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 1030(a)(5)(A) | Computer Fraud |
| 18 U.S.C. § 371 | Conspiracy to Commit Computer Fraud |

The application is based on these facts:

See Affidavit

☑ Continued on the attached sheet.

□ Delayed notice of _____ days *(give exact ending date if more than 30 days:* ________ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ John A. Maser
*Applicant's signature*

John A. Maser, Special Agent, FBI
*Printed name and title*

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 1/25/2023

Joi Elizabeth Peake
*Judge's signature*

City and state: Winston-Salem, North Carolina

Joi Elizabeth Peake, United States Magistrate Judge
*Printed name and title*

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH ONE INTERNET PROTOCOL ADDRESS THAT IS STORED AT PREMISES CONTROLLED BY GODADDY.COM, LLC | Case No. 1:23MJ42 |

## AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, John A. Maser, a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

### INTRODUCTION

1. The United States is investigating the Emotet malicious software ("malware") and botnet. I make this affidavit in support of an application for a search warrant for information associated with Internet Protocol ("IP") address 192.155.110.18 (the "Subject IP Address") that is stored at premises owned, maintained, controlled, or operated by GoDaddy.com, LLC ("GoDaddy"), a web hosting company headquartered at 2155 E. GoDaddy Way, Tempe, Arizona under the GoDaddy.com brand Velia.net / Realhosters.ru. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require GoDaddy to

disclose to the government records and other information in its possession, including content, pertaining to the subscribers or customers operating the Subject IP Address. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other witnesses and agents, including foreign law enforcement officers. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(5)(A) (computer fraud) and 371 (conspiracy to commit computer fraud) have been committed in the Middle District of North Carolina and elsewhere. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes further described in Attachment B.

## Agent Background

4. I am a Special Agent with the Federal Bureau of Investigation and have been since March 21, 2004. I am currently assigned to the Cyber Squad

in the Raleigh Resident Agency of the Charlotte Division. I have had this assignment since November 2014. Prior to this assignment, I was a Supervisory Special Agent assigned to the National Cyber Investigative Joint Task Force in Chantilly, Virginia. I have also been assigned to the Philadelphia Division where I investigated public corruption and the Cincinnati Division where I investigated white collar crime matters. Prior to becoming a Special Agent, I was employed as a CPA with an international accounting firm. I have previously conducted Federal criminal investigations involving the use of subpoenas, search warrants, and computer forensic examinations. I am an "investigative or law enforcement officer" within the meaning of 18 U.S.C. § 2510(7); that is, an officer of the United States of America who is empowered to investigate and make arrests for offenses alleged in this warrant.

## JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## STATUTORY AUTHORITY

6. Title 18, United States Code, Section 1030(a)(5)(A) provides that whoever "knowingly causes the transmission of a program, information, code,

or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished as provided in subsection (c) of this section." Section 1030(e)(2)(B) defines a "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]" Section 1030(e)(8) defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information[.]"

7. Title 18, United States Code, Section 371 provides: "If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both."

## PROBABLE CAUSE

### A. Overview of the Emotet Malware and Botnet

8. Emotet has targeted critical industries worldwide, including banking, e-commerce, healthcare, academia, government, and technology. Emotet malware has primarily infected victim computers through spam email messages containing malicious attachments or hyperlinks. Once it has infected

a victim computer, Emotet is typically used to deliver additional malware to the infected computer, such as ransomware or malware that steals financial credentials. The computers infected with Emotet malware are part of a botnet (i.e., a network of compromised computers), meaning the perpetrators can remotely control all the infected computers in a coordinated manner. The owners and operators of the victim computers are typically unaware of the infection.

9. In 2017, the computer network of a school district in the Middle District of North Carolina was infected with the Emotet malware. The Emotet infection caused damage to the school's computers, including but not limited to the school's network, which was disabled for approximately two weeks. In addition, the infection caused more than $1.4 million in losses, including but not limited to the cost of virus mitigation services and replacement computers.

10. From 2017 to January 2021, numerous other victims throughout North Carolina and the United States were infected with Emotet malware, to include computer networks of local, state, tribal, and federal governmental units, corporations, and networks related to critical infrastructure.

11. In January 2021, the FBI and international law enforcement agencies took steps to disrupt the Emotet malware and botnet. As part of this effort, Ukrainian law enforcement seized electronic devices from an Emotet server administrator. Other conspirators were not searched.

12. In November 2021, security researchers and the FBI observed Emotet malware being widely distributed for the first time since the international disruption efforts. The malware appeared to be an updated version of Emotet, based on unique code overlap and functionality. The Emotet spam operations ceased in July 2022 and resumed again in early November 2022.

### B. Continuation of the Emotet Conspiracy

13. In late February and early March 2022, the Twitter account @ContiLeaks publicly posted the contents of chat communications amongst various cybercriminals, including some members of the Emotet conspiracy. The chats, which date back to June 2020, were conducted through the communications platform Jabber and were hosted on a Tor onion service.

14. Based on a review of the chats, FBI and security researchers have assessed that the communications are authentic. The chats contain, for example, several discussions that include the following externally-corroborated distinctive characteristics: cryptocurrency transactions that are reflected on the publicly available blockchain; victims that were contemporaneously compromised by malware variants other than Emotet; nicknames and biographical information of known cybercriminals; details relating to the tactics, techniques, and procedures of malicious cybercriminal activity; and server and account information, such as Internet Protocol

addresses and email accounts, which other FBI investigations have confirmed were associated with malicious cybercriminal activity.

15. FBI's review of the leaked chat communications has shown that at least one Emotet conspirator has consistently administered the malware and botnet, including during the time periods before the January 2021 law enforcement action and after Emotet's November 2021 return. That, together with the unique code overlap and functionality of Emotet malware before and after the international disruption, has led FBI to conclude that the Emotet conspiracy continued through the disruption period to the present.

### C. The Subject IP Address

16. Prior to the law enforcement action in January 2021, administrators of the Emotet botnet used a system of tiered servers, described here as Tier 1, Tier 2, and Tier 3, to communicate with the Emotet malware installed on infected computers. Tier 1 servers were typically compromised web servers belonging to what appeared to be unknowing third parties. Tier 2 and Tier 3 servers were rented and controlled by the perpetrators. The primary function of the Tier 1 and Tier 2 servers was to forward communications containing encrypted data between infected computers and Tier 3 servers.

17. Since Emotet activity resumed in November 2021, based on publicly-reported cybersecurity research and the FBI's investigation, the Emotet administrators appear to be relying on a similar multi-tiered

infrastructure, with at least one additional tier, to communicate with and control victim computers infected with Emotet malware. Tiering of servers is used to obfuscate the identity of the perpetrators accessing the top tier of servers.

18. A confidential human source ("CHS"), as well as cybersecurity researchers, recently observed the Subject IP Address functioning as a new server for the Emotet botnet. On January 10, 2023, a researcher observed that Emotet bots began receiving new malware module updates after a long period of inactivity. Based on a review of past information provided by the CHS and these cybersecurity researchers, FBI views the current information as trustworthy and reliable. From the traffic associated with the module updates, researchers were able to identify the Subject IP Address. Researchers observed eleven known Tier 1 servers communicating with this new server and observed Emotet traffic flow over the server until January 16, 2023. The server is suspected to be compromised and, thus, it may belong to an unknowing third party.

19. As previously described, the primary function of lower tier servers is to forward communications containing encrypted data between infected computers and higher tiered servers. Traffic from this newly identified server located at the Subject IP Address was delivering module updates. Specifically,

this server was delivering malware loader and credential stealing modules to Emotet victims.

20. According to publicly available Whois records, the Subject IP Address—192.155.110.18—is hosted by GoDaddy. GoDaddy is assigned the IP block 192.155.96.0/20, which contains 4,096 IP addresses in the range 192.155.96.0–192.155.111.255. A sub-allocation of this block of IP addresses is held by Velia.net / Realhosters.ru. This sub-allocation block consists of the eight IP addresses in the range 192.155.110.16–192.155.110.23, which includes the Subject IP Address. Velia states, on its website beneath its logo, that the company is a "GoDaddy brand." According to publicly available whois records, the physical server hosting the Subject IP Address is located in the United States.

21. On January 11, 2023, pursuant to 18 U.S.C. § 2703(f), I requested that GoDaddy preserve the information on the server associated with the Subject IP Address.

22. Based on the information described above, there is probable cause to believe that the Subject IP Address has been used to commit and facilitate the commission of violations of 18 U.S.C. § 1030(a)(5)(A) (computer fraud) and 371 (conspiracy to commit computer fraud). In my training and experience, in the context of this investigation, the server that hosts the Subject IP Address is not only property used to commit a crime, but is also likely to contain

computer code and other data controlled by the Emotet administrators, which may help identify victims infected with Emotet malware and conspirators who have accessed the control panel in furtherance of the conspiracy. The server may also contain a historical record of the IP addresses of other servers used in furtherance of the offenses.

### BACKGROUND CONCERNING WEB HOSTING COMPANIES

23. Web hosting companies, such as GoDaddy, maintain server computers connected to the Internet. A server is a computer, which provides services to other computers. Hosting company customers use those servers for various functions, depending on the services offered by the hosting company, including to store and share various electronic files, execute applications, and operate websites on the Internet. Some hosting companies offer simple cloud storage, which allows the user to store files, much like an extra external hard drive, and sometimes share and edit those files with other persons. Other hosting companies allow users to operate and host websites on the Internet. Other hosting companies allow users to operate a virtual private server, or VPS, which allows the customer to run different virtualized operating systems, much like a virtual machine, through the user's computer through the Internet. A hosting company can offer any combination of the above.

24. GoDaddy advertises on its website that it offers several of these services, including web hosting; virtual private servers; and cloud hosting.

25. Hosting companies, such as GoDaddy, offer various "subscriptions" for the various services they offer for a regularly charged fee. Based on the type of service a customer needs, the customer selects the "subscription" and creates an account with the hosting company for those services. After a customer selects a subscription plan with the hosting company, often the customer can also select the physical location where data will be stored. The hosting company then hosts the subscriber's data at that physical location or locations. GoDaddy currently manages several data center locations, including data centers in the United States in Arizona, California, Illinois, and Virginia, and overseas in the Netherlands and Singapore.

26. A subscriber to a hosting company can manage and perform administrative tasks relating to the account with the hosting company by logging into the hosting company's administrative interface from a desktop, tablet, or mobile device. GoDaddy offers its customers an administrative dashboard or panel that allows users to monitor and manage one or more accounts at a time, including to monitor their central processing unit load average, memory usage, and disk usage; and to manage, add, and remove Secure Shell ("SSH") keys, which are described further below. Each subscriber to a hosting company's services has full administrative control over his account, which enables the subscriber to choose to install software from a menu the hosting company offers or store and run the subscriber's own software.

27. Hosting companies' customers can place files (sometimes even automatically synchronizing files in the cloud with files stored locally on the client's electronic devices), programming code, databases, and other data on computer servers controlled by the web hosting company. To do this, a customer can connect from their own computer to the server across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a website interface offered by the hosting company or via a mobile application. It is frequently possible for a customer to directly access the server computer through the SSH or Telnet protocols. These protocols allow remote users to type commands to the server. The SSH protocol can additionally be used to copy files to the server. A customer can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the IP addresses of the remote user's computer(s). IP addresses are used to identify computers connected to the Internet. Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

28. In general, hosting companies like GoDaddy ask each customer to provide certain personal identifying information when registering for an account. This information can include the customer's full name, physical address, telephone number and other identifiers, email addresses, and business information. In addition, for a paying customer, hosting companies typically retain information about the customer's means and source of payment for services (including any credit card or bank account number).

29. Hosting companies also typically retain certain information about the customer's use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files and data that reflect usage of the account.

30. In some cases, a subscriber or user will communicate directly with the hosting company about issues relating to a website or account, such as technical problems, billing inquiries, or complaints from other users. Hosting companies typically retain records about such communications, including records of contacts between the user and the company's support services, as well records of any actions taken by the company or user as a result of the communications.

31. As further described in Attachment B, this application seeks permission to obtain an image of the data associated with the Subject IP Address from the server that hosts  the Subject IP Address, rather than logical copies of the files stored on the server(s). A logical copy is simply a copy of a file, including any associated metadata, as it appears on a computer, but does not include any deleted data. An image, on the other hand, is a bit by bit duplicate of the server, including all files, slack space, memory, and metadata which can help establish how the account was used, the purpose of their use, who used them, and when. Logical copies typically do not require technical expertise to view, while an image often requires a technical expert to review, extract, and analyze the data.

32. The data stored on a web hosting account can be deleted by the user at any moment, and often are deleted or otherwise altered by users who are actively trying to conceal their activities from law enforcement. However, based on my training and experience, I know that computer files or remnants of such files—including those stored or used on a web hosting account—can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. This is the case because when a person "deletes" a file on a computer, the data contained in the "deleted" file actually remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may still reside

in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

33. Apart from user-generated files, computer storage media contain electronic evidence of how a web hosting account has been used, what it has been used for, and who has used it. To give a few examples, this evidence can take the form of operating system configurations, data from operating system or application operation, file system data structures, RAM and virtual memory "swap" or paging files. For instance, along with RAM, virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Computer file systems can record information about the dates files were created and sequence in which they were created.

34. In summary, based on my training and experience in this context, I believe that the computers of GoDaddy are likely to contain user-generated content such as electronically stored information (including the content of a web hosting account), as well as GoDaddy-generated information about its subscribers and their use of GoDaddy services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the

account's user or users. In fact, even if a subscriber provides GoDaddy with false information about identity, that false information often nevertheless provides clues to identity, location, or illicit activity.

35. As explained above, information stored in connection with a GoDaddy account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the investigating authorities to establish and prove each element of the offense or, alternatively, to exclude the innocent from further suspicion. From my training and experience, a user's IP address logs, stored electronic communications, and other data retained by GoDaddy, can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, contact information may indicate who used or controlled the account at a relevant time. Further, account activity can show how and when the account was accessed or used. For example, as described above, GoDaddy logs the IP addresses from which its subscribers access their accounts, along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of account access, use, and events relating to the crime

under investigation. Last, account activity may provide relevant insight into the account subscriber's state of mind as it relates to the offense under investigation. For example, information on the GoDaddy account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

## Conclusion

36. I submit that this affidavit supports probable cause for a warrant to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes further described in Attachment B.

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

38. Because the warrant will be served on GoDaddy, who will then be responsible for compiling the requested records at a time convenient to GoDaddy, reasonable cause exists to support execution of the requested warrant at any time day or night.

Respectfully submitted,

/s/ John A. Maser
John A. Maser
Special Agent
Federal Bureau of Investigation

1:23MJ42

Dated: January 25, 2023

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.

Joi Elizabeth Peake

Joi Elizabeth Peake
United States Magistrate Judge
Middle District of North Carolina

## ATTACHMENT A
## PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following Internet Protocol address that are stored at premises owned, maintained, controlled, or operated by GoDaddy.com, LLC, a web hosting company headquartered at 2155 E. GoDaddy Way, Tempe, Arizona under the GoDaddy.com brand Velia.net / Realhosters.ru:

192.155.110.18

## ATTACHMENT B
## PARTICULAR THINGS TO BE SEIZED

### I. Information to be disclosed by GoDaddy.com, LLC under the GoDaddy.com brand Velia.net / Realhosters.ru ("Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of Provider, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) (such a request was made by the Federal Bureau of Investigation on January 11, 2023), Provider is required to disclose the following information to the government associated with the Internet Protocol ("IP") address listed in Attachment A:

a. all records or other information pertaining to the IP address, including all files, databases, and database records stored by Provider in relation to that IP address or identifier;

b. a forensic image or snapshot of all data and information associated with the IP address electronically stored on the server or droplets, including memory and deleted files, that host the IP address;

c. all information in the possession of Provider that might identify the subscribers related to that IP address, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

d. all records pertaining to the types of service utilized by the user of the IP address; and

e. all records pertaining to communications between Provider and any person regarding the IP address, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of issuance of this warrant.

## II. Information to be seized by the government

All information described above in Section I, for each IP address listed in Attachment A, that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)(5)(A) (computer fraud) and 371 (conspiracy to commit computer fraud) in the form of the following:

1. Records and information revealing, referencing, or constituting the operation of the Emotet malware and botnet;

2. Records and information revealing or referencing persons who either collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation, or communicated

about matters relating to the criminal activity under investigation, including records that help reveal their location;

3. Records and information revealing and referencing how and when the server associated with the IP address was accessed or used as part of the operation of the Emotet malware and botnet;

4. Transactional and location information pertaining to any items authorized to be seized under this section (Section II);

5. All bank records, checks, credit card bills, account information, and other financial records used to carry out the criminal activity under investigation;

6. Files, databases, and database records stored by Provider referencing, revealing, or constituting the operation of the Emotet malware and botnet;

7. Subscriber information related to the account(s) established to host the IP address in Attachment A, to include:

   a. Names, physical addresses, telephone numbers and other identifiers, email addresses, and business information; and

   b. Length of service (including start date), types of service utilized, means and source of payment for services (including any credit card or bank account number), and billing and payment information.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, a complete copy of the disclosed electronic data may be delivered to the custody and control of attorneys for the government and their support staff for their independent review.